# МЕТОД ОЦЕНИВАНИЯ КВАНТОВОЙ УСТОЙЧИВОСТИ БЛОКЧЕЙН-ПЛАТФОРМ

***Петренко А.С.[1], Петренко С.А.[2]***

***Цель работы:*** *разработка нового метода оценивания квантовой устойчивости современных блокчейн-платформ на основе результативного решения задач криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS), базирующихся на вычислительно трудных задачах факторизации и дискретного логарифмирования.*

***Метод исследования:*** *использование квантовых алгоритмов, предоставляющих экспоненциальный выигрыш (например, алгоритма Шора) и квадратичный выигрыш (например, алгоритма Гровера). В связи с тем, что класс задач, решаемых квантовыми алгоритмами за полиномиальное время, пока не удается существенно расширить, в работе большее внимание уделено криптоанализу на основе квантового алгоритма Шора и других полиномиальных алгоритмов.*

***Результаты исследования:*** *построена классификация известных алгоритмов и пакетов программ криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS), основывающихся на вычислительно трудных задачах факторизации и дискретного логарифмирования. Предложен перспективный метод решения задач криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) известных блокчейн-платформ за полиномиальное время в квантовой модели вычислений. Разработаны алгоритмы решения задач квантового криптоанализа схем двухключевой криптографии известных блокчейн-платформ за полиномиальное время с учетом стойкости дискретного алгоритма (DLP) и дискретного алгоритма с эллиптической кривой (ECDLP). Спроектирована структурно-функциональная схема программного комплекса квантового криптоанализа современных блокчейн-платформ «Квант-К», адаптированного под работу в гибридной вычислительной среде квантового компьютера IBM Q (20 и 100 кубит) и Супер-ЭВМ IBM BladeCenter (2022). Разработана методика применения программного комплекса «Квант-К» для оценивания квантовой устойчивости блокчейн-платформ: InnoChain (Innopolis University), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), NodesPlus (b41), Мастерчейн (Сбербанк), Microsoft Azure Blockchain, Enterprise Ethereum Alliance и др.*

***Научная и практическая значимость*** *результатов статьи состоит в выработке решения для вычислительно трудных задач факторизации и дискретного логарифмирования, заданных над конечными коммутативными (и некоммутативными) ассоциативными алгебрами, в квантовой модели вычислений за полиномиальное время. Существенно, что полученные научные результаты легли в основу разработки соответствующего программно-аппаратного комплекса «Квант-К», который был апробирован в гибридной вычислительной среде (квантовый компьютер IBM Q (20 и 100 кубит) и/или Супер-ЭВМ 5 поколения: IBM BladeCenter (2022), РВС на ПЛИС Virtex UltraScale (2020), ВС РФЯЦ-ВНИИЭФ (2022) и СКИФ П-0.5 (2021). Разработана и апробирована соответствующая методика оценивания квантовой устойчивости названных блокчейн-платформ на основе авторских моделей, методов и алгоритмов квантового криптоанализа.*

***Ключевые слова:*** *технологии блокчейна и распределенного реестра (DLT), SMART контракты, модель угроз безопасности блокчейн, квантовая угроза безопасности, криптографические атаки, квантовый криптоанализ, квантовая и пост-квантовая криптография, квантовые алгоритмы алгоритмы Шора, Гровера и Саймона, квантовое преобразование Фурье, задача факторизации и дискретного логарифмирования, пост-квантовая криптография, квантовая устойчивость блокчейн-платформ.*

**DOI:** 10.21681/2311-3456-2022-3-2-22

1 Петренко Алексей Сергеевич, исследователь по направлению 10.06.01 «Информационная безопасность» ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)», Санкт-Петербург, Россия. orcid.org/ 0000-0002-9954-4643, E-mail: A.Petrenko1999@rambler.ru

2 Петренко Сергей Анатольевич, профессор кафедры информационной безопасности (ИБ), доктор технических наук, профессор ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)», Санкт-Петербург, Россия. orcid.org/0000-0003-0644-1731, E-mail: S.Petrenko@rambler.ru

## Введение

В настоящее время технологии блокчейн получили широкое распространение во всем мире. Например, глобальные корпорации *IBM, J.P. Morgan, Amazon* и др. интегрировали упомянутые технологии в свои базовые программнотехнические решения, а *Facebook* даже анонсировала собственную криптовалюту *Libra*. В России большее развитие получили блокчейн-платформы: *InnoChain (Innopolis University), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), NodesPlus (b41), Мастерчейн (Сбербанк), Microsoft Azure Blockchain, Enterprise Ethereum Alliance* и др. Одной из причин популярности блокчейн-технологий стала принципиальная возможность отказаться от услуг некоторой доверенной третьей стороны для организации безопасной передачи данных [1-6,9]. Современные блокчейн-платформы состоят из ряда независимых узлов, которые достигают так называемого консенсуса перед обновлением соответствующих реестров новыми транзакциями. При этом известно несколько механизмов достижения консенсуса, среди которых более распространен *Proof-of-Work (PoW)*. Следует констатировать, что применение механизмов консенсуса и криптографических примитивов (см. табл. 1) уже недостаточно для нейтрализации квантовой угрозы и обеспечения требуемой квантовой устойчивости блокчейн-платформ. Здесь под *квантовой устойчивостью* понимается некоторое системное свойство блокчейн-платформы, интуитивно определяемое как *способность сохранять постоянство (неизменность) упомянутой платформы* и ее ключевых системных свойств в условиях криптографических атак с использованием квантовых компьютеров [14,15,19,29,38,39].

Дело в том, что квантовые компьютеры способны решать некоторые вычислительные задачи значительно эффективнее любого современного классического компьютера (СуперЭВМ 5 поколения) *архитектуры фон Неймана*. Наиболее выразительными и интересными, с прикладной точки зрения, примерами таких задач является факторизация целого числа, эффективно выполняемая квантовым *алгоритмом Шора*, а также поиск записи в неупорядоченной базе данных, эффективно решаемый *алгоритмом Гровера* [10-12, 16-18, 26-28, 32-41].

В 1994 г. американский математик *Питер Шор (Peter Shor)* разработал алгоритм, который позволяет

*Таблица 1*

*Характеристика объекта исследования*

| Криптовалюта | Электронная подпись | Параметры | Алгоритм консенсуса | Регулировка сложности | Целевой интервал времени блокировки |
|---|---|---|---|---|---|
| **Bitcoin** | ECDSA | Secp256k1 | Proof of Work | Отсутствует | 10 мин. |
| **Litecoin** | ECDSA | Secp256k1 | Proof of Work | Отсутствует | 2,5 мин. |
| **Namecoin** | ECDSA | Secp256k1 | Proof of Work | Детерминированное обязательство | 10 мин. |
| **Dogecoin** | ECDSA | Secp256k1 | Proof of Work | Отсутствует | 1 мин. |
| **Primecoin** | ECDSA | Secp256k1 | Proof of Work | Сложность регулируется в каждом блоке | 1 мин. |
| **Auroracoin** | ECDSA | Secp256k1 | Proof of Work | Каждые 8 блоков | 1 мин. |
| **Dash** | ECDSA | Secp256k1 | Proof of Work | Механизм DGW | 2,5 мин. |
| **Vertcoin** | ECDSA | Secp256k1 | Proof of Work | В каждом блоке | 2,5 мин. |
| **Ethereum** | ECDSA | Secp256k1 | Proof of Work | Отсутствует | 15 сек. |
| **Zcash** | ECDSA<br>EDDSA | Secp256k1 (по умолчанию)<br>Ed25519 (защищённый вариант) | Proof of Work | Отсутствует | 75 сек. |
| **Bitcoin Cash** | ECDSA | Secp256k1 | Proof of Work | Экстренная регулировка сложности | 10 мин. |

решить задачу факторизации за полиномиальное время (стало быть, полиномиально количество гейтов) и на полиномиальном количестве кубитов, в то время как классические алгоритмы решают её за суперполиномиальное (субэкспоненциальное) время. А это значит, что квантовый компьютер с достаточным количеством кубитов подвергает криптографические примитивы блокчейн-платформ угрозе компрометации. Алгоритм Шора отличается от других известных квантовых алгоритмов в части наличия серьёзной прикладной значимости и является более сложным с точки зрения математики и архитектуры. Для его реализации задействованы две вычислительные парадигмы — классическая часть готовит входные данные для алгоритма Шора, а также управляет циклами и возвратами в целях нахождения требуемого результата; квантовая часть исполняет линейную последовательность унитарных преобразований над специально подготовленными состояниями входных кубитов [32-41].

Суть алгоритма факторизации Шора заключается в сведении задачи факторизации к задаче поиска периода функции. Если известен период функции, то упомянутая факторизация осуществляется при помощи алгоритма Евклида за полиномиальное время на классическом компьютере. Квантовая часть алгоритма факторизации как раз и занимается поиском периода функции. А классическая часть алгоритма сначала специальным образом готовит оную функцию, а потом проверяет найденный квантовой частью период на достаточность для решения задачи. Если период найден правильно (алгоритм вероятностный, так что может найти не то, что требуется), то задача решена. Если же нет, то квантовая часть алгоритма прогоняется ещё раз. А, поскольку, проверка правильности решения для задачи факторизации достаточна проста (умножение двух чисел и сравнение с третьим), то эту часть алгоритма можно не учитывать при подсчёте сложности. Следует признать, что среди известных квантовых алгоритмов (которых более 40), *алгоритм Шора* более известен, и, можно даже утверждать, что из-за упомянутого алгоритма, новая вычислительная модель, основанная на законах квантовой механики, получила такое широкое развитие. Всё дело в том, что именно на гипотезе алгоритмической сложности задачи факторизации числа основаны многочисленные современные алгоритмы и системы криптографии.

Существенно, что квантовый алгоритм Шора позволяет решать задачи факторизации и дискретного логарифмирования, и может быть использован для криптоанализа большинства практически применимых криптосистем (*RSA, DSA, ECDSA, ГОСТ Р 34.10*). Ожидается, что в ближайшие пять лет квантовые компьютеры превзойдут классические компьютеры *архитектуры фон Неймана* в решении задачи криптоанализа. В том числе, криптоанализа криптосистемы *RSA* (одной и самых распространенных систем асимметричного шифрования, названной в честь ее авторов *– Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman)).* К 2025 году квантовые компьютеры смогут эффективно взламывать RSA с длиной ключа 2048 битов (минимально рекомендуемой международными криптографическими стандартами) [11-25, 29-32, 40, 41].

На данный момент при помощи *алгоритма Шора* на квантовых компьютерах успешно факторизованы числа *15=3*5 и 21=3*7* (https://research-information.bris.ac.uk/en/publications/experimental-realization-of-shors-quantum-factoring-algorithm-usi). Также для решения задачи факторизации был успешно адаптирован *4-кубитовый адиабатический* квантовый компьютер, факторизовавший число *143=11*13* (https://arxiv.org/pdf/1111.3726v1.pdf) и число *56153=233*241* (https://arxiv.org/abs/1411.6758). Любопытно, что факторизация большего числа сперва осталась незамеченной исследователями, и лишь спустя два года было показано, что в ходе эксперимента был факторизован целый класс чисел. Далее, методом квантового отжига на компьютере *D-Wave 2X* было факторизовано *число 200099* (https://arxiv.org/abs/1604.05796). Следующим интересным результатом стала факторизация числа *291311* (https://www.researchgate.net/scientific-contributions/Richard-Tanburn-2079794789) при помощи квантового компьютера, основанного на принципах ядерного магнитного резонанса. А рекордным факторизованным числом на текущий момент времени является число *1099551473989=1048589*1048601* (https://4627su41pzrvhaad34118k3y-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/Analyzing-the-Performance-of-Variational-Quantum-Factoring-on-a-Superconducting-Quantum-Processor.pdf).

Таким образом, развитие алгоритмической базы способно сократить сроки появления эффективных квантовых вычислителей в течении 5 лет. Более того, перспективы появления «практического» квантового компьютера, способного выполнять поставленные задачи криптоанализа, становятся еще ближе, если учитывать результаты компании *IBM* по разработке квантовых процессоров. Так, в ноябре 2021 года

*IBM представила 127-кубитовый процессор Eagle*, а к 2023 году прогнозирует преодоление *1000-кубитового* предела (https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor). В свое время, исследователями компании *Google* было показано, что для эффективного криптоанализа RSA достаточно порядка *20 000 000* физических (доступных на текущем уровне технологии) кубитов (https://arxiv.org/pdf/1905.09749.pdf). С учетом возможности эффективного распараллеливания вычислений между несколькими устройствами с существенно меньшим числом кубитов, продемонстрированной в указанной работе, достижения IBM убедительно свидетельствуют о реалистичности реализации квантовой угрозы. Поэтому в ряде стран, главным образом в США и Евросоюзе запланирован в течение 2022-2025 гг. переход к устойчивой *квантовой (пост-квантовой) криптографии* (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-175b.pdf). Так, упомянутый NIST находится в процессе разработки стандартов квантовой криптографии, а АНБ рекомендует своим поставщикам внедрить SHA-384 вместо SHA-256.

### Вербальная и математическая задача исследования

*Вербальная постановка задачи.*

**Дано:**

Схемы асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) (см. табл. 6) исследуемых блокчейн-платформ: *InnoChain (Innopolis University), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), NodesPlus (b41), Мастерчейн (Сбербанк), Microsoft Azure Blockchain, Enterprise Ethereum Alliance* и др.

**Необходимо:**

Повысить результативность квантового криптоанализа систем асимметричного шифрования и цифровой

*Таблица 2*

*Характеристика криптографических примитивов объекта исследования*

| **Стандарт (криптосистемы и криптопримитивы)** | **Возможные каналы связи** | **Объем (от возможных 100%)** |
|---|---|---|
| **Алгоритм RSA** с длиной ключа 1024 2048 4096 | Блокчейн-сети Internet Intranet IIoT/IoT Спутниковые сети | ~25% |
| **Алгоритм RSA-OAEP** | Блокчейн-сети Internet Intranet IIoT/IoT Спутниковые сети | ~35% |
| **Алгоритм Эль-Гамаля** над группой точек эллиптической кривой | Блокчейн-сети Internet Intranet IIoT/IoT Спутниковые сети | ~35% |
| **ECDLP** NIST P-256 NIST P-256 NIST P-256 | Блокчейн-сети Internet Intranet IIoT/IoT Спутниковые сети | |
| Протоколы **TLS, SSH, IPSec** (полагаются на соглашения о ключах Диффи-Хеллмана и зависят от стойкости дискретного алгоритма (DLP) и дискретного алгоритма с эллиптической кривой (ECDLP) | Internet Intranet | ~98% |

| Стандарт (криптосистемы и криптопримитивы) | Возможные каналы связи | Объем (от возможных 100%) |
|---|---|---|
| Цифровые подписи **DSA, ECDSA, RSA-PPS** | Блокчейн-сети Internet Intranet | ~75% |


*Рис. 1. Область гарантированного решения задачи квантового криптоанализа криптопримитивов блокчейн-платформ с требуемой результативностью*

подписи исследуемых блокчейн платформ с учетом стойкости дискретного алгоритма (DLP) и дискретного алгоритма с эллиптической кривой (ECDLP) в зависимости от:

- трудоемкости алгоритма криптоанализа систем асимметричного шифрования и цифровой подписи;
- имеющихся реальных вычислительных ресурсов (квантовый компьютер или симулятор на классическом компьютере, количества логических и физических кубитов, уровней глубины моделируемой квантовой схемы, показателей стабильности квантового вычислителя, характеристик производительности компьютера в целом);
- значения вероятности взлома системы асимметричного шифрования и цифровой подписи.

*Математическая постановка задачи*

**Исходные данные:**

- Структура схемы асимметричного шифрования (*RSA, Эль-Гамаля*) и/или цифровой подписи (*DSA, ECDSA или RSA-PSS*) исследуемых блокчейн-платформ *InnoChain (Innopolis University), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), NodesPlus (b41), Мастерчейн (Сбербанк), Microsoft Azure Blockchain, Enterprise Ethereum Alliance* и др.;
- Приложения и/или протоколы (*TLS, SSH и IPSec*).

**Набор ограничений:**

- Ограничения на *W* — значение показателя трудоемкости алгоритма криптоанализа (*в сек.*) схемы асимметричного шифрования (*RSA, Эль-Гамаля*) и/или цифровой подписи (*DSA, ECDSA или RSA-PSS*);
- Ограничения на *N* — временные и вычислительные ресурсы для проведения криптоатаки (допустимый период времени на криптоатаку, тип компьютера — квантовый компьютер или симулятор на классическом компьютере, количество логических и физических кубитов, количество уровней глубины моделируемой кванто-

*Таблица 3*

*Характеристика стойкости криптосистем и криптопримитивов исследуемых блокчейн-платформ*

| Для оценивания компонентов криптосхемы | Для оценивания криптосхемы в целом |
|---|---|
| Способствует | Возможен |
| Не влияет | Затруднен |
| Затрудняет | Существенно затруднен |
| Делает невозможным | Невозможен |

вой схемы, значения показателей стабильности функционирования квантового вычислителя в условиях когеренции, значения показателей производительности компьютера в целом);

— Ограничения по значению *P* — вероятности успешно проведенной криптоатаки на схему асимметричного шифрования (*RSA, Эль-Гамаля*) и/или цифровой подписи (*DSA, ECDSA или RSA-PSS*).

**В результате анализа требуется найти:**

— Числовую комплексную оценку, характеризующую стойкость схемы асимметричного шифрования (*RSA, Эль-Гамаля*) и/или цифровой подписи (*DSA, ECDSA или RSA-PSS*) исследуемых блокчейн-платформ к квантовым алгоритмам криптоанализа (под успешным выполнением криптоанализа понимается восстановление секретного ключа шифрования или получение возможности дешифровать сообщение без изначального знания секретного ключа)

$$F_{\sum} = \sum_{i=1}^{s} f_i\left(W, N, P_{def}\right), F_{\sum} \geq F_{def}, \text{где } F_{def} -$$

эталонное значение,

$$f_i\left(W, N, P_{def}\right) =$$

$$= \begin{cases} 0, \forall W, N : P_{W,N} < P_{def} \\ 1, P_{W,N} \geq P_{def} \\ \dfrac{P_{def}}{\left(1+\dfrac{W'}{W}\right)\left(1+\dfrac{N'}{N}\right)}, P_{W,N} < P_{def}, \exists W', N' : P_{W',N'} \geq P_{def} \end{cases}$$

— Развернутую характеристику стойкости схем асимметричного шифрования (*RSA, Эль-Гамаля*) и/или цифровой подписи (*DSA, ECDSA или RSA-PSS*) к квантовым алгоритмам криптоанализа в виде табл. 3 содержащей нечеткие оценки из заданного множества.

## Предлагаемый метод оценки квантовой устойчивости блокчейн

Рассмотрим следующую типовую последовательность действий (рис. 2) для схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS):

1) на основе закрытого ключа *Абонента А* формируется открытый ключ;

2) открытый ключ передается *Абоненту Б*;

*3) Абонент Б* выполняет шифрование информации с помощью открытого ключа *Абонента А*;

*4) Абонент Б* передает шифртекст *Абоненту А* по каналу связи;

*5) Абонент А* выполняет расшифрование шифртекста с помощью своего закрытого ключа.

Тогда к базовым принципам, необходимым для решения поставленной задачи (подробно рассмотрены в работе авторов 19), следует отнести следующие:

1) Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. При этом механизм генерации является общеизвестным.

2) Имеются надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом. Механизм шифрования является общеизвестным.

3) Владелец двух ключей никому не сообщает закрытый ключ, но передает открытый ключ контрагентам или делает его общеизвестным.

Здесь под факторизацией натурального числа понимается его разложение в произведение простых множителей. Существование и единственность (с точ-

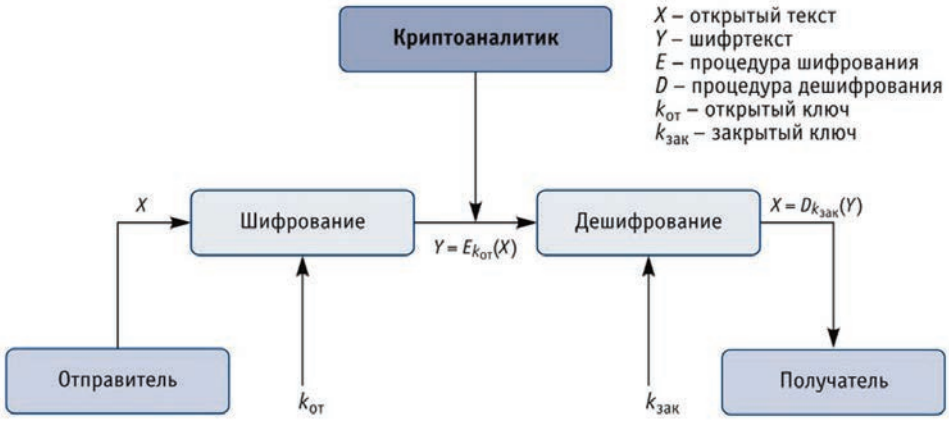



*Рис. 2. Типовая схема ассиметричного шифрования*

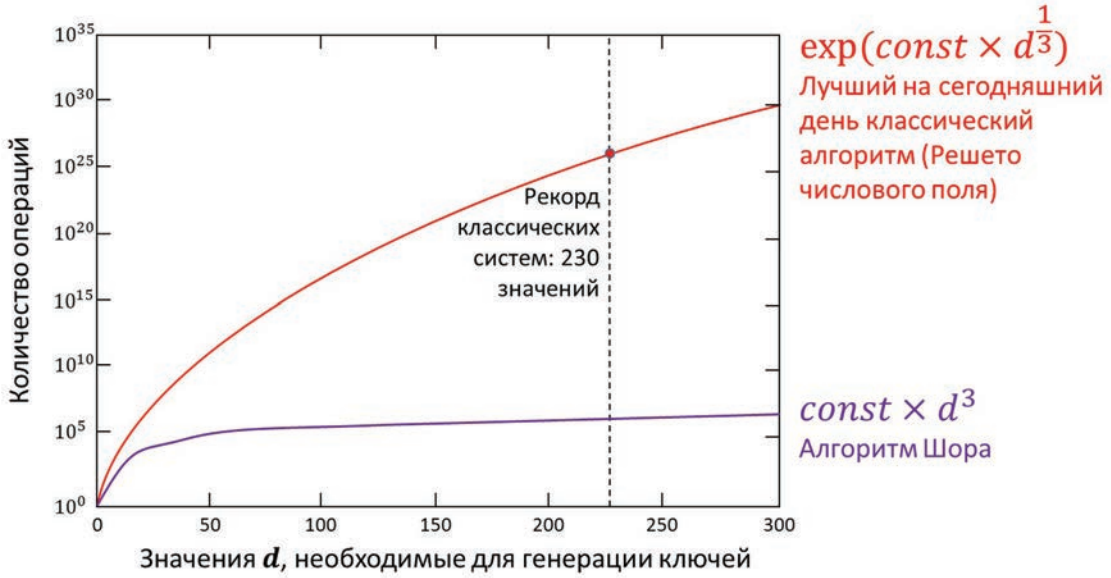



*Рис. 3. Пояснения к оценке стойкости исследуемых криптосистем*

ностью до порядка следования множителей) такого разложения следует из основной теоремы арифметики. В отличие от задачи распознавания простоты числа, факторизация предположительно является вычислительно сложной задачей. Поэтому здесь актуально нахождение эффективного квантового алгоритма факторизации целых чисел (рис. 3). При этом нет доказательств того, что решение этой задачи за полиномиальное время не существует.

Заметим, что предположение о том, что для больших чисел задача факторизации является вычислительно сложной, лежит в основе широко используемых алгоритмов. Решение ряда прикладных задач математики и теоретической информатики зависит от полноты, непротиворечивости и разрешимости упомянутой задачи факторизации. В том числе: применения *эллиптических кривых, алгебраическая теория чисел и квантовые вычисления и др*. Как правило, на вход таких алгоритмов подаётся число, которое необходимо факторизовать, состоящее из $N = \lfloor log_2 n \rfloor + 1$ символов (если $n$ представлено в двоичном виде). При этом сначала осуществляется поиск первого простого делителя, после чего, при необходимости, поиск повторяется для дальнейшей факторизации. Прежде чем начинать факторизацию большого числа, следует убедиться в том, что оно не простое. Для этого достаточно пройти соответствующий тест числа. Эта задача детерминировано разрешима за полиномиальное время.

В зависимости от сложности алгоритмы факторизации были разделены на две группы. В первую группу

*Таблица 4*

*Временная сложность алгоритмов, решающих задачи факторизации и дискретного логарифмирования*

| **Решение задачи факторизации** | |
|---|---|
| Название | Сложность |
| Метод Ферма | $T(N)=O(N^{\frac{1}{3}})$ |
| Метод Ленстры | $T=O(e^{\sqrt{2\ln p\ \ln\ln p}}$ ) |
| Метод Диксона | $T=O(L(n)^2)$ |
| Метод квадратичного решета | $T=O\left(\exp\left((1+o(1))\sqrt{\log n\log\log n}\right)\right)$ |
| Метод решета числового поля | $T(N)=O(n\log n\log N)$ |
| Метод Шора | $T=O(\log_3 M)$ |
| **Решение задачи дискретного логарифмирования** | |
| Название | Сложность |
| Метод Адлемана | $T=O\left(c^{\ln p^{\frac{1}{2}}}\right)$ |
| Метод COS | $T=O(\exp\left((\log p\log\log p)^{\frac{1}{2}}\right))$ |
| Метод решета числового поля | $T(N)=O(n\log n\log N)$ |
| Метод Шора | $T=O(\log_3 M)$ |

вошли *экспоненциальные алгоритмы*, сложность которых экспоненциально зависит от длины входящих параметров (то есть от длины *N* самого числа в бинарном представлении). Во вторую группу — *субэкспоненциальные алгоритмы*. Понятно, что стойкость алгоритмов симметричной и асимметричной криптографии основывается на сложности решения определенных классов задач на классических компьютерах (*перебор, факторизация и дискретное логарифмирование* лежат в классе сложности *NPP* по длине ключа в битах), в противоположность квантовой криптографии, стойкость которой основывается на законах квантовой физики. Оценка временной сложности основных алгоритмов факторизации и дискретного логарифмирования представлены в табл. 4.

Таким образом, типовые схемы асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) основываются на сложности вычисления дискретного логарифма в конечных группах, определенных над различными алгебраическими конструкциями, или на сложности разложения натурального числа на простые сомножители. А степень уязвимости упомянутых схем базируется на вычислительной сложности факторизации чисел [6-19,32,40,41].

Заметим, что задачи дискретного логарифмирования и факторизации имеет асимптотическую сложность при решении на квантовом компьютере $O\left(n^2\log n\log\log n\right)$ квантовых шагов. На классическом компьютере с использованием лучшего из известных алгоритмов — алгоритма решета числового поля — асимптотическая сложность составляет $O\left(e^{cn^{1/3}\log^{2/3}n}\right)$, где $c$ - некоторая константа. Полиномиальное решение задач дискретного логарифмирования на квантовом компьютере находится также за $O\left(n^2\log n\log\left(\log n\right)\right)$.

В результате, практическая значимость квантовых алгоритмов решения задач факторизации и дискретного логарифмирования заключается в том, что с их помощью при использовании квантового компьютера с несколькими сотнями логических кубитов (см. рис. 5 – рис. 7) становится возможным взлом криптографических систем с открытым ключом. Например, *RSA* использует открытый ключ $M$, являющийся произведением двух больших простых чисел. Один из способов взломать шифр *RSA* - найти его множители. При достаточно большом $M$ это практически невозможно сделать, используя известные классические алгоритмы. Лучший из известных классических алгоритмов факторизации требует времени порядка $M^{1/3}$.

1. $|0\rangle|0\rangle$ -Инициирование состояния

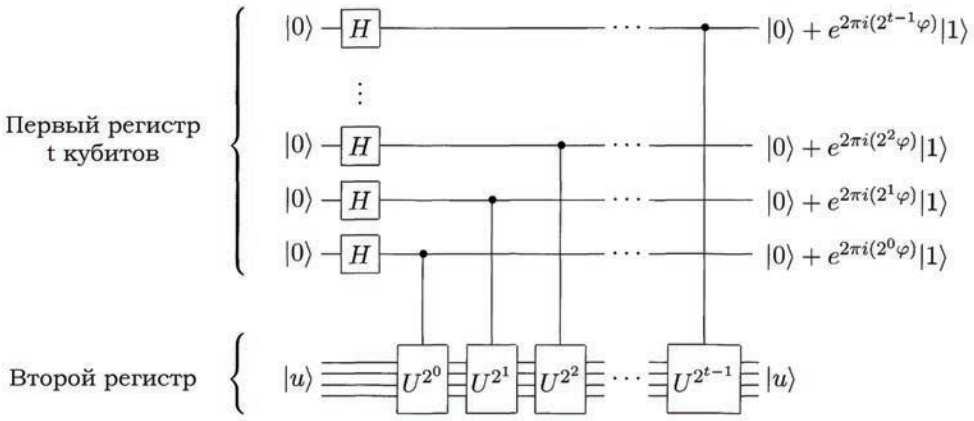
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |0\rangle\ |0\rangle$ -Создание суперпозиции

3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |0\rangle\ |f(x)\rangle$ -Применить U $f(x) = ax(mod\ N)$

$\approx \frac{1}{\sqrt{r2^t}} \sum_{l=0}^{r-1} \sum_{x=0}^{2^t-1} |0\rangle|f(x)\rangle$

4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{l/r}\rangle\ |\hat{f}(l)\rangle$ -Применить QFT (квантовое преобразование Фурье) к первому регистру

*Рис. 5. Основные этапы квантового алгоритма факторизации Шора*




Чтобы получить f (n-битное число) с вероятностью успеха $1-\varepsilon$ необходимо следующее число кубит:

$$t = n + \left\lceil \log(2 + \frac{1}{2\varepsilon}) \right\rceil$$

*Рис. 6. Нахождение необходимого количества кубитов, как критерия успешности решения задачи криптоанализа*

*Алгоритм Шора*, используя возможности квантовых компьютеров, способен произвести факторизацию числа не просто за полиномиальное время, а за время, ненамного превосходящее время умножения целых чисел (то есть практически так же быстро, как происходит само шифрование) [32-41].

Понятно, что здесь идет речь не только о *схеме RSA*, прямо опирающейся на сложности факторизации, но и о других сходных схемах асимметричного шифрования (производные от RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS), которые становятся уязвимыми.

## Разработка платформы «Квант-К»

Для инженерной реализации предлагаемого нового метода оценивания квантовой устойчивости исследуемых блокчейн-платформ сначала определим ряд функциональных и технических требований.

$$f(x) = a^x mod\ N.$$

$$7^4 mod\ 15 \equiv 1 \Rightarrow 7^4 - 1\ mod\ 15 \equiv 0 \Rightarrow (7^2-1)(7^2+1)\ mod\ 15 \equiv 0\ mod\ 15 \Rightarrow$$
$$\Rightarrow 48 * 50 \text{ делится без остатка на } 15$$

$N = 15$ $\quad \gcd(48,15) = 3$ $\quad \gcd(50,15) = 5$

$x = 7$

$t = 11$ $\quad \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|0\rangle = \frac{1}{\sqrt{2^t}} [|0\rangle + |1\rangle + |2\rangle + \ \dots\ + |2^t - 1\rangle]|0\rangle$

$\varepsilon = 1/4$

$$f(k) = x^k mod\ N$$

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|x^k mod\ N\rangle = \frac{1}{\sqrt{2^t}} [|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \ \dots]$$

*Рис. 7. Пример квантового решения задачи факторизации*

*Функциональные требования к платформе «Квант-К»:*

— Платформа должна осуществлять криптоанализ схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) исследуемых блокчейн-платформ путем экспоненциального ускорения решения задач факторизации, дискретного логарифмирования (DLP) и дискретного логарифмирования с эллиптической кривой (ECDLP). В том числе, широко распространенных протоколов TLS, SSH и IPSec, полагающихся на соглашения о ключах Диффм-Хелмана (зависят от стойкости DLP или ECDLP), цифровые подписи (DSA, ECDSA или RSA-PSS) или на шифрование с открытым ключом (Эль-Гамаль, RSA-OAEP).

— Платформа должна быть ориентирована на работу с пользователями различной квалификации в области криптоанализа (оператор, администратор, прикладной и системный программист, криптоаналик средней и высшей категории).

— Подготовку данных для криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) должен осуществлять отдельный модуль.

— Подготовку данных для выводов результатов криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) и сохранения в специальных базах данных SQL и/или NoSQL типов должен осуществлять отдельный модуль.

— Процедуру криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) должен осуществлять отдельный модуль.

— Платформа должна осуществлять вывод информации о результатах криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS).

— Платформа должна обеспечивать возможность сохранения результатов криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) для дальнейшей их аналитической обработки и использования.

— Платформа должна быть универсальной и иметь возможности для дальнейшей доработки и усовершенствования.

*Технические требования к платформе «Квант-К»:*

— Платформа должна работать на классических компьютерах архитектуры фон Неймана и демонстрационных прототипах квантового компьютера IBM Q с 16, 20, 100 и более логическими кубитами.

— Платформа должна быть реализована на основе следующих программных архитектур: *моно-*

*лит, двух и трех-звенная клиент-серверная SOA, микросервисная*.

- Платформа должна быть независима от конкретной реализации облачных вычислений (Amazon Web Services, Azure от Microsoft, Google App Engine, Rackspace, Force.com от компании Salesforce, Intuit Partner Platform, Facebook, IBM Cloud, VMWare vCloud, Sharepoint Online, Red Hat OpenShift Container Platform).
- Платформа должна поддерживать единый стек программирования (Python, Go, Scala, C++, .Net, Data Science, AI и ML)
- Платформа должна работать под управлением операционных систем (ОС) семейства MS Windows и Linux (Astra Linux).
- Платформа должна поддерживать открытое ПО, а также известные библиотеки моделирования квантовых алгоритмов и пакеты программ с длинной арифметикой.
- Должен быть предусмотрен функциональный API для развития и улучшения программного комплекса в будущем.

*Также при разработке перспективной платформы «Квант-К» учитывалось следующее.*

*Во-первых,* квантовый алгоритм факторизации Шора характеризуется вероятностной природой [32-37,40,41]. Здесь первый источник случайности встроен в классическое вероятностное сведение разложения на множители к нахождению периода некоторой функции. Второй источник появляется из необходимости наблюдения квантовой памяти, которое также выдаёт случайные результаты. Поэтому, были запрограммированы следующие шаги решения задачи факторизации:

1) Выбор случайного остатка *a* по модулю *N*.
2) Проверка *НОД(a, N) = 1*.
3) Нахождение порядка *r* остатка *a* по модулю *N*.
4) Если *r* четен, вычислено *НОД*( $a^{r/2} - 1, N$).

Здесь (с большой вероятностью) полученное на четвертом шаге число всегда являлось нетривиальным делителем $N$. Достаточно трудным шагом для реализации оказался третий шаг. Здесь минимальное $r$ такое, что а $r \equiv 1 mod\ N$ порядок $a$ по модулю $N$ (*порядок* $r$ является периодом функции $f(x) = a\,x\,mod\,N$). Например, пусть есть число $N$. Будем случайно подбирать число *a* так, чтобы оно было взаимно-простым с $N$. Такое число найдется с большой вероятностью. Повторив несколько раз, найдем такое число (число $a$ называется взаимнопростым к $b$, если их наибольший общий делитель равен 1). После этого определим порядком $r$ остатка $a$ по модулю $N$. Получим: $a^r \equiv 1 mod\ N$. Мы хотим, чтобы $r$ было четным. Если это не так, вернемся к шагу выбора числа $a$. Итак, имеем: $a\,r \equiv 1 mod\ N$, где $r$ — четно, тогда можно написать: $(a^{r/2} - 1)\left(a^{r/2} + 1\right) = cN$, где $c$ — некоторое целое положительное число. Нетрудно доказать, что одна из скобок имеет с $N$ общий нетривиальный делитель. Тогда, взяв $gcd\left(a^{r/2} - 1, N\right)$, получим один делитель $N$ (может получиться, что общий нетривиальный делитель число $N$ будет иметь со второй скобкой, тогда мы вновь должны будем повторить выбор числа $a$). Разделив $N$ на полученное число, находим второй делитель. Задача разложения числа $N$ на множители, свелась к быстрому нахождению периода *r* для случайно подобранного числа $a$.

*Во-вторых*, для определения периода функции $r$ с помощью преобразования *Фурье* не потребовалось вычислять все значения $f(x)$. Задача свелась к решению, похожему на решение задачи *Дойча* [32-37,30,41], в которой учитываются не все значения функции, а только некоторые её свойства. В результате, полученные представления *Фурье-преобразования* в форме произведения (рис. 8) позволили промоделировать требуемые квантовые цепи (рис. 9) для работы с квантовым компьютером IBM Q, который был выбран для инженерной реализации и апробации предложенного квантового алгоритма факторизации Шора (рис. 10).

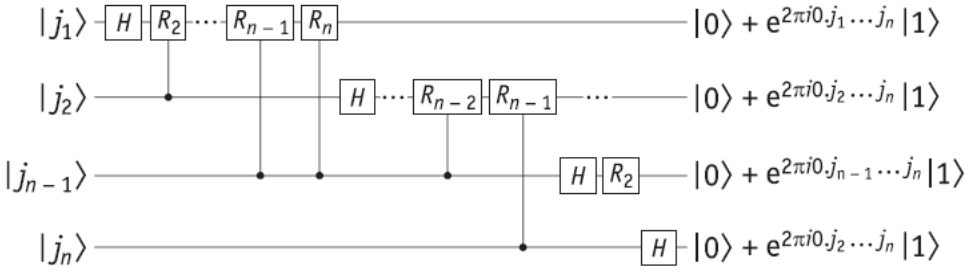



*Рис. 8. Гейтовое представление квантового преобразования Фурье*

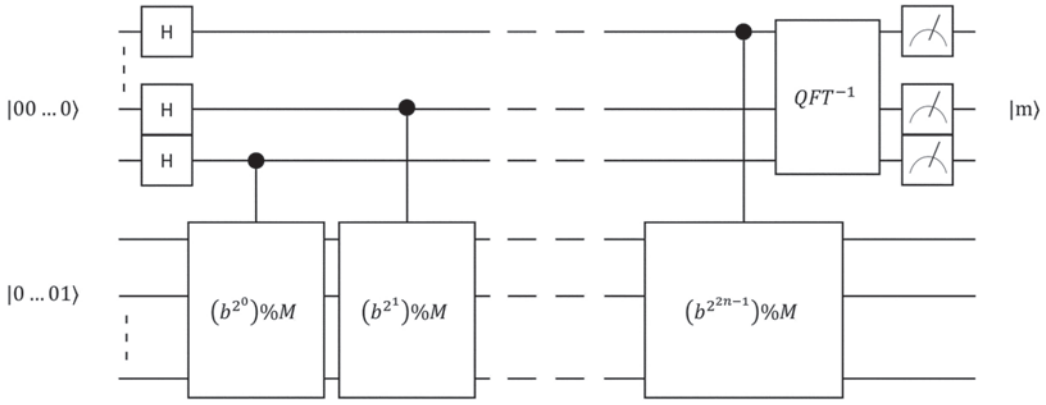



*Рис. 9. Квантовое представление модифицированного алгоритма факторизации Шора*

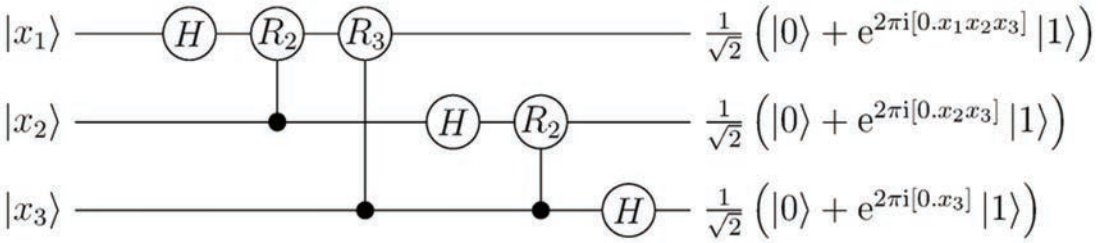



*Рис. 10. Пример моделирования квантового гейта*

Здесь *гейт* $R_k$ обозначает унитарное преобразование вида:

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

*В-третьих,* была опробована схема прямого подключения к квантовой (16, 20 и 100-кубитной системе *IBM Q)* с помощью платформы *IBM Cloud.* Для этого был получен прямой доступ к *IBM Quantum Experience и осуществлен з*апуск соответствующее приложения (рис. 11) на квантовой схеме для работы с отдельными кубитами.

*В-четвертых*, были апробированы возможные гибридные схемы из квантовых вычислителей *IBM Q* и симуляторов на суперЭВМ пятого поколения (СуперЭВМ Ломоносов-2, Торнадо, СКИФ, вычислители на ПЛИС). При этом были задействованы приложения автора на языке *Python*, а также ряд открытых библиотек для моделирования квантовых алгоритмов на квантовых схемах [19].

В состав авторской платформы «Квант-К» вошли следующие программные модули (рис. 12):

1) Модуль первичного анализа криптосистемы, предназначенный для определения криптографического шифра и сведения задачи вскрытия к задаче факторизации;

2) Модуль поиска периода неопределённой функции, предназначенный для реализации факторизации на квантовой вычислительной системе;

3) Модуль расчёта секретного ключа, предназначенный для обработки полученного в результате функционирования предыдущего модуля результата факторизации для последующего вскрытия криптосистемы;

4) Модуль представления результатов и их анализа, предназначенный для отображения полученного результата и анализа характеристик его получения.

При этом структурно-функциональная схема платформы «Квант-К» представлена на рис. 12.

А основной алгоритм работы платформы «Квант-К» приведен на рис.13.

Отметим, что для разработки платформы «Квант-К» был использован язык программирования *Python* с применением интерпретатора *Jupyter Notebook* (входит в пакет разработки *Anaconda*), а также библиотеки *Qiskit* IBM.

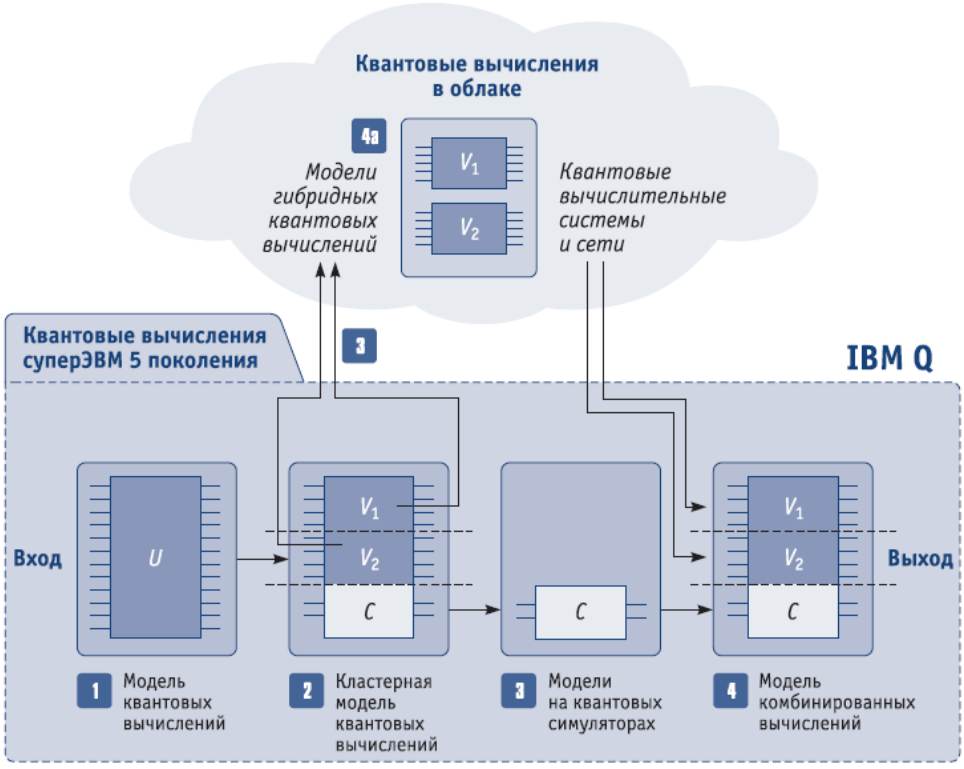



*Рис. 11. Апробация разработанной платформы «Квант-К» в среде IBM Q System One (16, 20 и 100-кубит) и суперЭВМ 5 поколения*

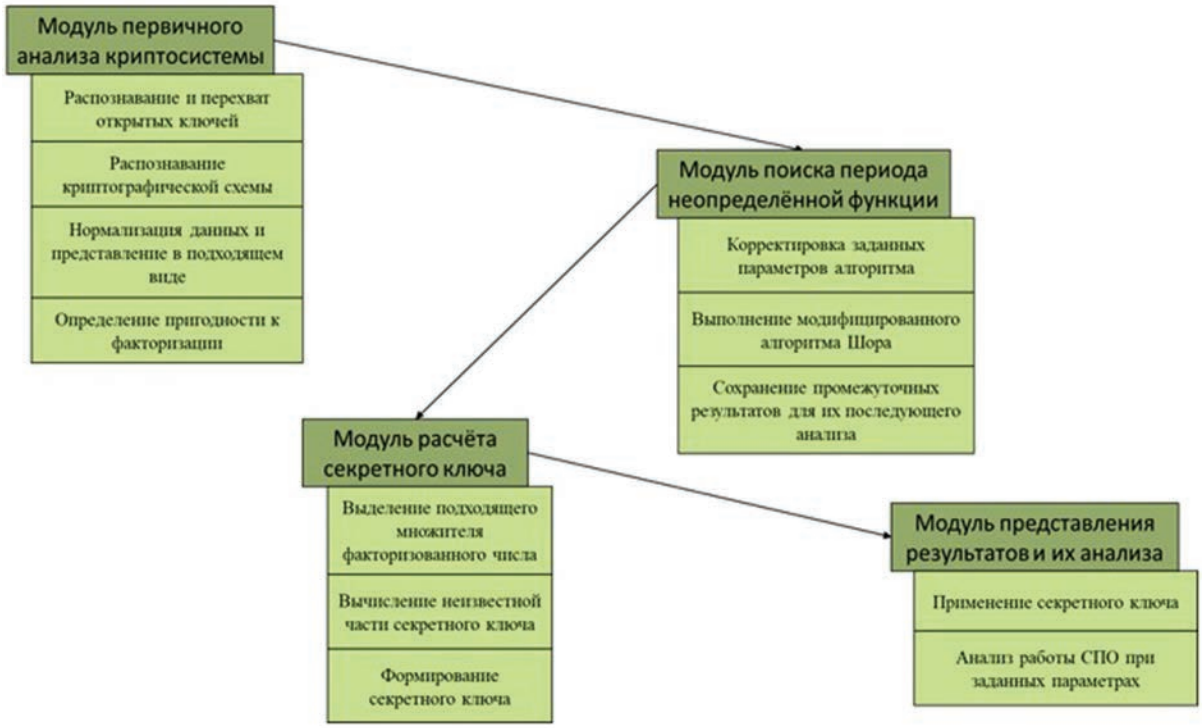



*Рис.12. Структурно-функциональная схема платформы «Квант-К»*

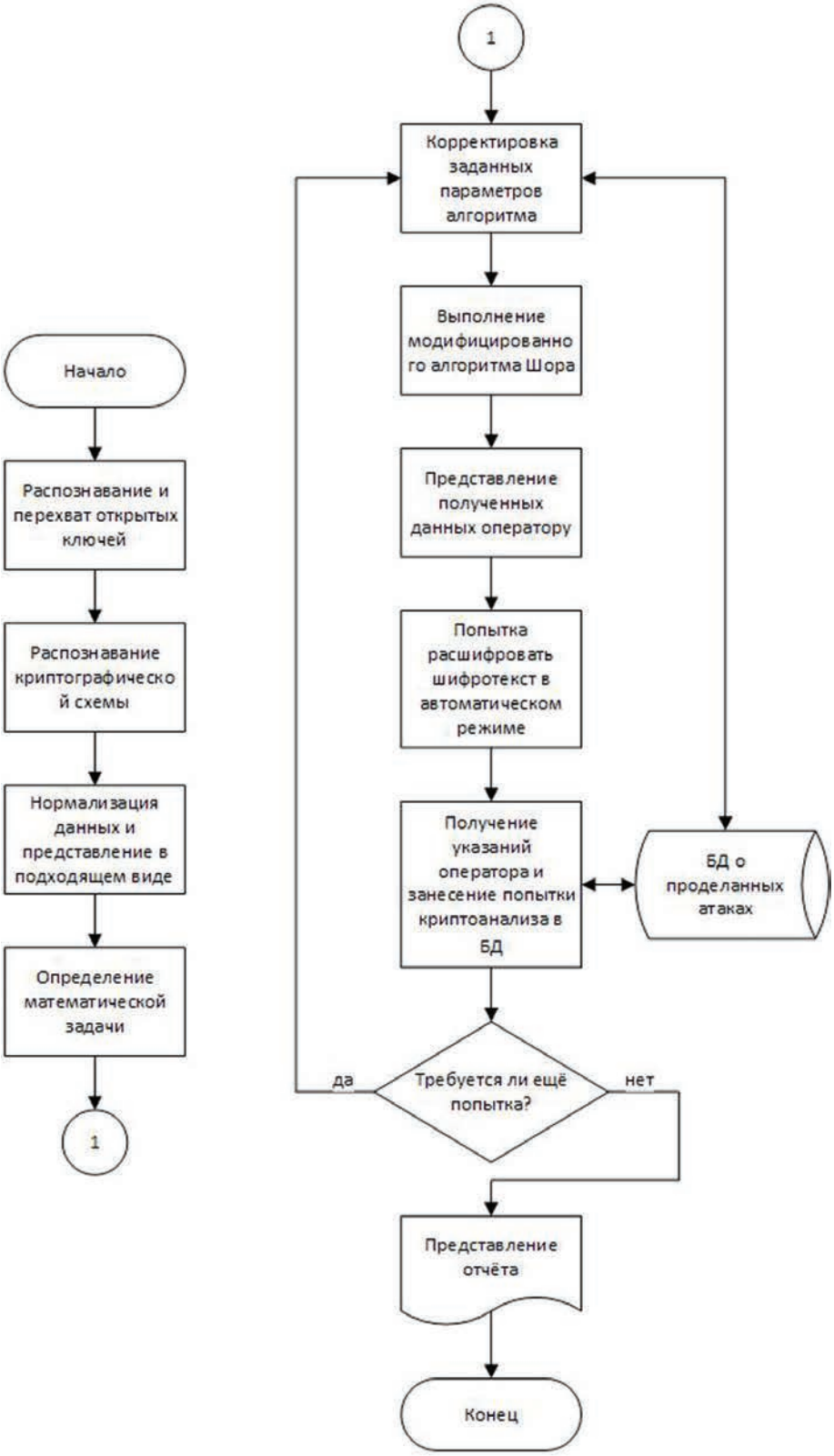



*Рис. 13. Блок-схема алгоритма работы «Квант-К»*

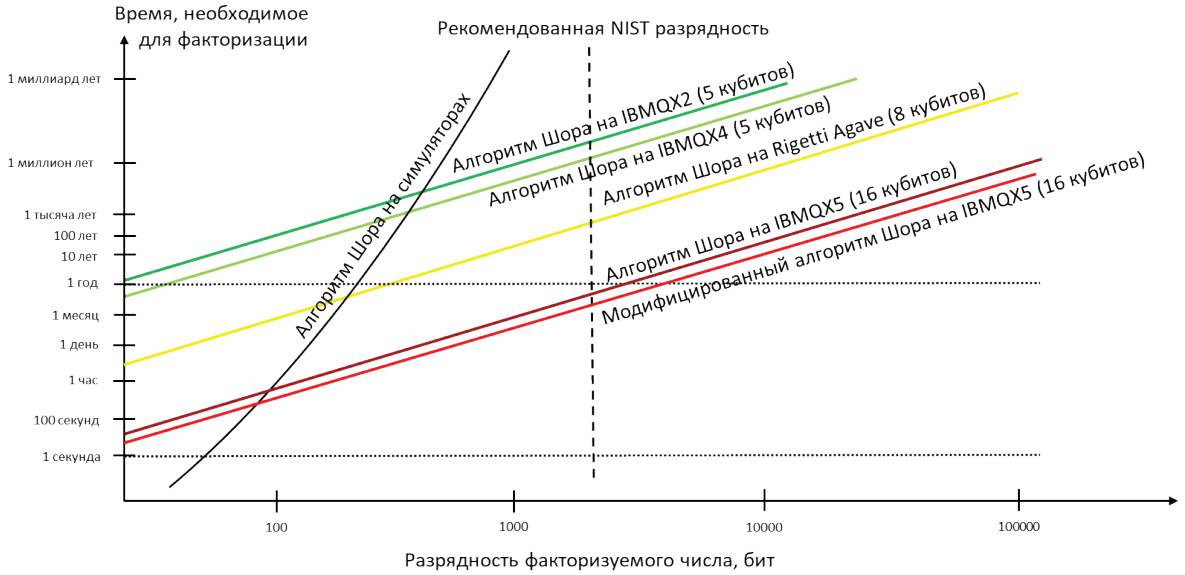



*Рис. 14. Суммарный выигрыш от предлагаемой квантовой Реализации алгоритма Шора в гибридной среде IBM Q и СуперЭВМ пятого поколения*

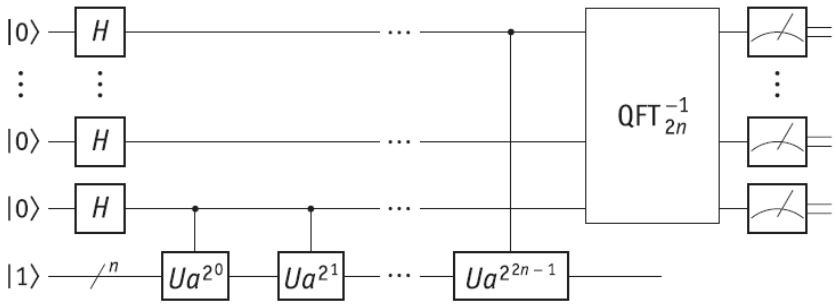



*Рис.15. Представления квантового алгоритма Шора для гибридной среды IBM Q и СуперЭВМ пятого поколения*

К достоинствам авторской платформы «Квант-К» (см. рис. 18) можно отнести следующее.

1. Впервые для оценивания квантовой устойчивости известных блокчейн-платформ был предложен и обоснован новый вид квантового криптоанализа схем асимметричного шифрования (*RSA, Эль-Гамаля*) и цифровой подписи (*DSA, ECDSA или RSA-PSS*) на основе модифицированного авторами статьи алгоритма факторизации Шора.

2. Повышение оперативности исследования криптостойкости схем асимметричного шифрования (*RSA, Эль-Гамаля*) и цифровой подписи (*DSA, ECDSA или RSA-PSS*) исследованных блокчейн платформ на 20%-30% за счет автоматизации первой и второй части модифицированного (квантового) алгоритма факторизации Шора в гибридной среде IBM *Q* (16, 20, 100 и более кубитов) и СуперЭВМ пятого поколения (рис. 17).

3. Увеличение доли квантовых алгоритмов криптоанализа в арсенале инструментальных средств криптоанализа схем асимметричного шифрования (*RSA, Эль-Гамаля*) и цифровой подписи (*DSA, ECDSA или RSA-PSS*) до 17% (рис.18).

4. Повышение результативности криптоанализа асимметричных шифров схем асимметричного шифрования (*RSA, Эль-Гамаля*) и цифровой подписи (*DSA, ECDSA или RSA-PSS*) исследованных в работе блокчейн-платформ на 10-15% в целом.

## Заключение

Анализ вероятностных характеристик квантовых преобразований Фурье и Шора свидетельствует о

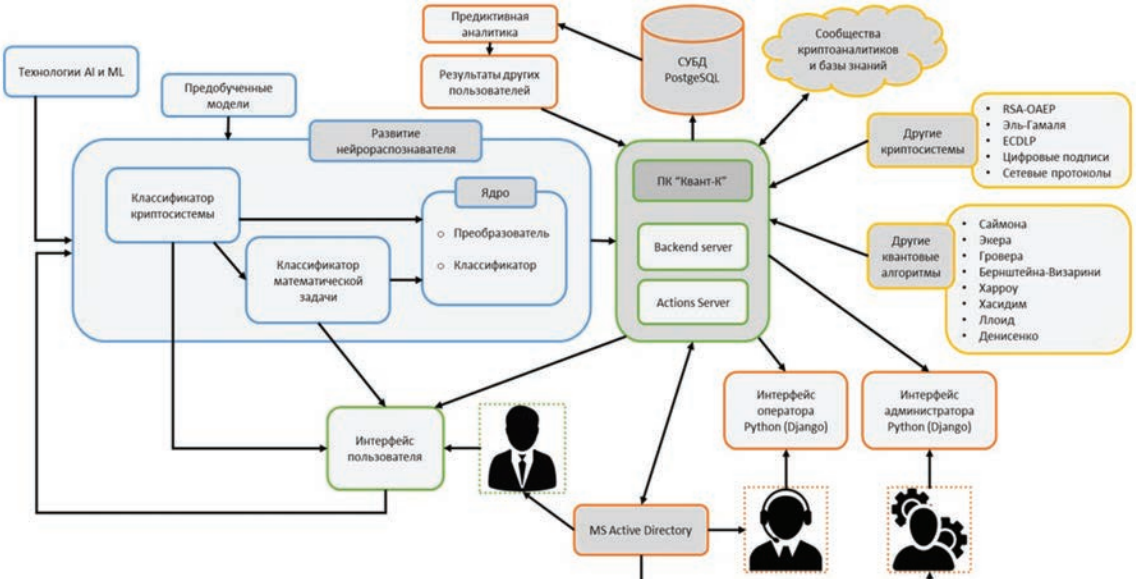



*Рис. 16. Перспективная архитектура платформы квантового криптоанализа «Квант-К»*

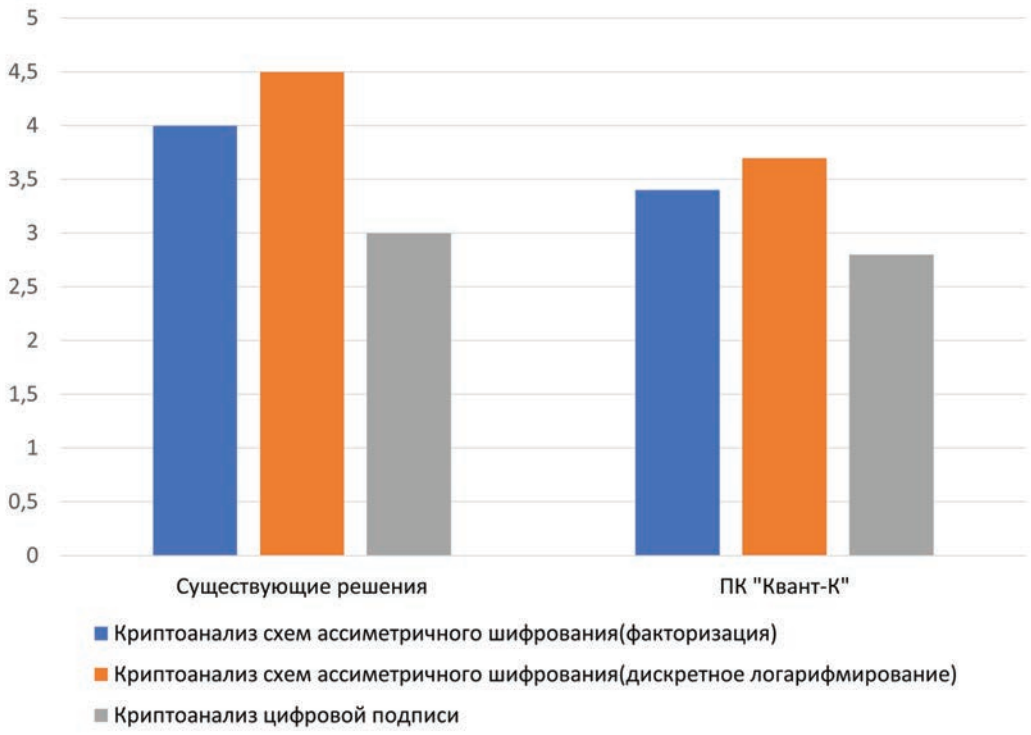



*Рис. 17. Сравнительный анализ времени криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS) блокчейн-платформ*

существенном квантовом ускорении решения задач криптоанализа схем асимметричного шифрования (*RSA, Эль-Гамаля*) и цифровой подписи (*DSA, ECDSA* или *RSA-PSS*) современных блокчейн-платформ, основанных на факторизации натуральных чисел и дискретном логарифмировании в конечных группах различной математической природы.

Пример решения задачи факторизации и дискретного логарифмирования в квантовой модели вычислений показал, что существует возможность перевода упомя-


*Рис. 18. Увеличение доли квантовых алгоритмов криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS)*

нутых задач из неполиномиального класса сложности в полиномиальный класс. Это существенно для повышения вероятности вскрытия систем асимметричного шифрования и цифровой подписи, а также криптографических примитивов в приложениях и протоколах (TLS, SSH и IPSec), получивших широкое распространение в известных блокчейн-платформах: *InnoChain (Innopolis University), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), NodesPlus (b41), Мастерчейн (Сбербанк), Microsoft Azure Blockchain, Enterprise Ethereum Alliance* и др.

Оценка сложности квантового алгоритма факторизации Шора с учетом стойкости дискретного алгоритма (DLP) и дискретного алгоритма с эллиптической кривой (ECDLP) позволила определить необходимые и достаточные условия для успешного решения поставленных задач исследования, подробно рассмотренных в настоящей статье. Была сформулирована соответствующая концептуальная и математическая постановки задачи исследования.

Анализ предельных возможностей известных моделей алгоритма факторизации Шора на квантовой схеме позволил сформулировать функциональные и технические требования к разрабатываемым перспективным квантовым алгоритмам криптоанализа схем асимметричного шифрования (*RSA, Эль-Гамаля*) и цифровой подписи (*DSA, ECDSA* или *RSA-PSS*) для блокчейн-платформ. В том числе, для авторской платформы «Квант-К», разработанной в ходе апробации предлагаемого нового метода оценивания квантовой устойчивости известных блокчейн-платформ. Отметим, что на авторскую платформу «Квант-К» было получено Свидетельство о регистрации программы для ЭВМ № 2020665981в 2021 году.

К возможным направлениям дальнейшего развития авторской платформы «Квант-К» можно отнести следующее:

— Снижение квантовой декогеренции путём использования специальных исправляющих алгоритмов, в том числе, на основе методов коррекции ошибок;
— Добавление в библиотеку платформы других квантовых и пост-квантовых алгоритмов (*Гровера, Саймона, Экера, Берштейна-Вазирани, Харроу, Хассилима, Ллойда, Денисенко, Ключкарева, Гребнева, Федотова, Чижова, Бельского и* др.);
— Совершенствование методов определения пригодности криптосистем для криптоатаки;
— Добавление в библиотеку «Квант-К» новых криптосистем блокчейн-платформ для криптоанализа;
— Развитие интерфейса платформы «Квант-К» для организации коллективной работы криптоаналитиков на основе облачных технологий (доступ к другим квантовым вычислительным системам, доступ к библиотекам с уязвимостями известных реализаций криптосистем и протоколов, доступ к библиотекам других реализаций квантовых алгоритмов) и мобильных технологий (социальные сети, мессенджеры, чаты и боты) и др.

*Статья подготовлена по результатам исследований, выполненных при поддержке гранта РФФИ (№ 20-04-60080)*

**Литература**


1. Богданов А.Ю. Квантовые алгоритмы и их влияние на безопасность современных классических криптографических систем. /А.Ю. Богданов, И.С. Кижватов // РГГУ. — 2005. — 18 с.
2. Валиев К.А. Квантовые компьютеры и квантовые вычисления / К.А. Валиев.-М.:Insitute of Physics and Technology, 2005.- 387с.
3. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М.: МЦНМО, 2003. – 328 с.
4. Гультяева Т. А. Основы теории информации и криптографии. — Новосибирск: Издательство НГТУ, 2010. — 88 с. — ISBN 978-5-7782-1425-5.
5. Денисенко Д.В., Маршалко Г.Б., Никитенкова М.В., Рудской В.И., Шишкин В.А. Оценка сложности реализации алгоритма Гровера для перебора ключей алгоритмов блочного шифрования ГОСТ Р 34.12-2015, Журнал экспериментальной и теоретической Физики, РАН, Институт физических проблем им. П.Л. Капицы РАН (Москва), 2019, том 155, вып. 4, стр. 645–653, 2019.
6. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления / М.: МЦНМО, Изд. ЧеРо, 1999. – 192 с.
7. Колмогоров, А.Н. Теория информации и теория алгоритмов. АН СССР. – М.: Наука, 1987.
8. Котельников В. А. Судьба, охватившая век. В 2 т. / сост. Н. В. Котельникова. М.: Физматлит, 2011. 312 с.
9. Корольков А.В. О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров. / А.В. Корольков // Вопросы кибербезопасности № 1(9) – 2015. – М.: Журнал «Вопросы кибербезопасности», 2015. – с. 6-13.
10. Ключарев П.Г. Автореферат диссертации на соискание кандидата технических наук. Алгоритмическое и программное обеспечение для моделирования квантового компьютера. МГТУ им. Н.Э. Баумана, 2009, 18 с.
11. Крэндалл Р., Померанс К. Простые числа: Криптографические и вычислительные аспекты / под ред. В. Н. Чубарикова ; пер. А. В. Бегунца [и др.]. — М. : УРСС: Книжный дом «ЛИБРОКОМ», 2011. — 664 с.
12. Манин Ю.И. Вычислимое и невычислимое. М.: Советское радио, 1980. 128 с.
13. Матвеев Е.А. Диссертация на соискание кандидата физико-математических наук. Применение квантовомеханических эффектов в системах защиты информации. Пенза, НТП Криптософт, 2019 – 157 с.
14. Молдовян А.А., Молдовян Н.А. Новые формы скрытой задачи дискретного логарифмирования. Труды СПИИРАН 2019. Том 18 №2. Стр. 504-529.
15. Молдовян Н.А., Введение в криптосистемы с открытым ключом /Молдовян Н.А., Молдовян А.А./, Изд. БХВ-Петербург, 2005, 286 с. — 2005.
16. Николенко С.И. Новые конструкции криптографических примитивов, основанные на полугруппах, группах и линейной алгебре. Диссертация на соискание кандидата физико-математических наук. СПб., Учреждение РАН Санкт-Петербургское отделение Математического института им. В.А. Стеклова РАН, 2008 – 120 с.
17. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ – М: Мир, 2006 г. – 824 с., ил.
18. Основы криптографии. Учебное пособие / А. П. Алферов [и др.]. — М. : Гелиос АРВ, 2001. — 480 с. — ISBN 5-85438-137-0.
19. Петренко, А.С., Романченко А.М. Перспективный метод криптоанализа на основе алгоритма Шора// Защита информации. Inside №2 2020. – СПб.: Изд. Афина, 2020. – с. 17–23.
20. Правильщиков П.А. Квантовый параллелизм и решение уравнений в задачах управления на базе новой модели вычислений / П.А. Правильщиков.- М.:Институт проблем управления им. В.А. Трапезникова, 2014.- 179 с.
21. Прескилл Дж. Квантовая информация и квантовые вычиселения / Д. Прескилл.-М.:Ижевск, 2008. — 464 с.
22. Ручкин В.Н. Естественный параллелизм квантовых компьютеров и нейровычислителей/ В.Н. Ручкин, В.А. Романчук, В.А. Фулин.- Рязань.:Рязанский государственный университет им. С.А. Есенина, 2013 – 387 с.
23. Сачков В.Н., В.А. Котельников и шифрованная связь. Конференции и симпозиумы, Т. 176, № 7, УФН 2006, с. 775-777
24. Словарь криптографических терминов. Под редакцией Б. А. Погорелова и В. Н. Сачкова. Московский государственный университет им. М.В. Ломоносова Академия криптографии Российской Федерации. Москва Издательство МЦНМО. 2006. – 50 с.
25. Токарева Н.Н. Об истории криптографии в России, Исторические очерки о дискретной математике и ее приложениям, №4 (18), Математический институт им. С.Л. Соболева СО РАН г. Новосибирск, 2012, — с. 82-107.
26. Холево А. С. Математические основы квантовой информатики – М.: МИАН, 2018. – 118 с. – (Лекц. курсы НОЦ, ISSN 2226-8782; Вып. 30). ISBN 978-5-98419-080-7
27. Холево А. С. Квантовые системы, каналы, информация. Электронное издание. М.: МЦНМО, 2014. — 327 с. ISBN 978-5-4439-2092-4
28. Холево А. С.. Введение в квантовую теорию информации. МЦНМО, 2002 – 128 с.
29. Черёмушкин А. В. Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика. — 2009. — нояб. — вып. 2. — с. 115—150. — URL: https: / / cyberleninka. ru / article / n / kriptograficheskie — protokoly-osnovnye-svoystva-i-uyazvimosti.pdf.
30. Шеннон К. Работы по теории информации и кибернетике / под ред. Р. Л. Добрушина, О. Б. Лупанова. — М. : Издательство иностранной литературы, 1963. — 830 с.
31. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходный код на языке С. Изд. Вильямс, 2016. – 816 с.

32. Shor P. Algorithms for quantum computation: discrete logarithms and factoring [Text] /Shor P.// Foundations of Computer Science.—1994.—№10. —134p.
33. Deutsch D., Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society A. 400 (1818), 97 — 117 (1985)
34. Deutsch D., Jozsa R., Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London A, 439, (1907), 553-558 (1992)
35. Diffie D, Hellman M. New directions in cryptography, IEEE Transactions on Information Theory, v. 22, Issue 6 (1976)
36. Feynman R, Simulating physics with computers, Internat. J. Theoret. Phys. 21, 467 — 488 (1982)
37. Grover L.K., A fast quantum mechanical algorithm for database search, In Proceedings of the twenty-eighth, annual ACM symposium on Theory of computing, 212 – 219, ACM (1996)
38. Markov A., Markov G., Tsirlov V. SIMULATION OF SOFTWARE SECURITY TESTS BY SOFT COMPUTATIONAL METHODS: CRITICAL INFRASTRUCTURES: CONTINGENCY MANAGEMENT, INTELLIGENT, AGENT-BASED, CLOUD COMPUTING AND CYBER SECURITY (IWCI 2019). Proceedings of the VIth International Workshop. Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences. 2019. С. 257-261.
39. Dorofeev A.V., Markov A.S., Tsirlov V.L. APPLICATION OF OPEN DATA IN ACCORDANCE WITH INFORMATION SECURITY REQUIREMENTS: CEUR Workshop Proceedings. ISTMC 2019 — Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation “Information Systems and Technologies in Modeling and Control”. 2019. С. 36-46.
40. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing 26, 1484 – 1509 (1997).
41. Simon D.R., On the power of quantum computation, SFCS ‘94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 116 – 123 (1994).

# QUANTUM RESILIENCE ESTIMATION METHOD BLOCKCHAIN

***Petrenko A.S.[3], Petrenko S.A.[4],***

***Abstract***

***Purpose of work*** *is the development of a new method for estimating the quantum resilience of modern blockchain platforms based on the effective solution of cryptanalysis problems for asymmetric encryption schemes (RSA, El-Gamal) and digital signature (DSA, ECDSA or RSA-PSS), based on computationally difficult problems of factorization and discrete logarithm.*

***Research method*** *is the use of quantum algorithms providing exponential gain (eg Shor’s algorithm) and quadratic gain (eg Grover’s algorithm). Due to the fact that the class of problems solved by quantum algorithms in polynomial time cannot yet be significantly expanded, more attention is paid to cryptanalysis based on the quantum Shor algorithm and other polynomial algorithms.*

***Results of the study*** *include a classification of well-known algorithms and software packages for cryptanalysis of asymmetric encryption schemes (RSA, El-Gamal) and digital signature (DSA, ECDSA or RSA-PSS) based on computationally difficult problems of factorization and discrete logarithm has been built. A promising method for solving problems of cryptanalysis of asymmetric encryption schemes (RSA, ElGamal) and digital signature (DSA, ECDSA or RSA-PSS) of known blockchain platforms in polynomial time in a quantum computing model is proposed. Algorithms for solving problems of quantum cryptanalysis of two-key cryptography schemes of known blockchain platforms in polynomial time are developed, taking into account the security of the discrete algorithm (DLP) and the discrete elliptic curve algorithm (ECDLP).*

*A structural and functional diagram of the software package for quantum cryptanalysis of modern blockchain platforms “Kvant-K”, adapted to work in a hybrid computing environment of the IBM Q quantum computer (20 and 100 qubits) and the IBM BladeCenter (2022) supercomputer, has been designed. A methodology has been developed for using the “Kvant-K” software package to assess the quantum stability of blockchain platforms:*

3 Alexei S. Petrenko, Postgraduate student in the direction 10.06.01 “Information Security” Saint-Petersburg State Electrotechnical University «LETI», Saint-Petersburg, Russia. Orcid.org/ 0000-0002-9954-4643, Email: A.Petrenko1999@rambler.ru

4 Sergei A. Petrenko, Dr.Sc. (in Tech.), Professor Saint-Petersburg State Electrotechnical University «LETI», Saint-Petersburg, Russia. Orcid.org/0000-0003-0644-1731, E-mail: S.Petrenko@rambler.ru

*InnoChain (Innopolis University), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), NodesPlus (b41), Masterchain (Sberbank), Microsoft Azure Blockchain, Enterprise Ethereum Alliance, etc.*

***Practical relevance:*** *The developed new solution for computationally difficult problems of factorization and discrete logarithm, given over finite commutative (and non-commutative) associative algebras, in a quantum model of computing in polynomial time. It is essential that the obtained scientific results formed the basis for the development of the corresponding software and hardware complex "Kvant-K", which was tested in a hybrid computing environment (quantum computer IBM Q (20 and 100 qubits) and/or 5th generation supercomputer: IBM BladeCenter (2022), RCS based on FPGA Virtex UltraScale (2020), RFNC-VNIIEF (2022) and SKIF P-0.5 (2021). An appropriate method for estimating the quantum stability of these blockchain platforms based on the author's models, methods and algorithms of quantum cryptanalysis has been developed and tested.*

***Keywords:*** *blockchain and distributed ledger technologies (DLT), SMART contracts, blockchain security threat model, quantum security threat, cryptographic attacks, quantum cryptanalysis, quantum and post-quantum cryptography, quantum algorithms Shor, Grover and Simon algorithms, quantum Fourier transform, factorization and discrete logarithm problem, post-quantum cryptography, quantum resilience of blockchain platforms.*

**References**

1. Bogdanov A.Yu. Quantum algorithms and their impact on the security of modern classical cryptographic systems /A.Yu. Bogdanov, I.S. Kizhvatov//RGGU. -2005.- 18 p.
2. Valiev K.A. Quantum computers and quantum computing / K.A. Valiev.-M.: Institute of Physics and Technology, 2005.- 387 p.
3. Vasilenko O. N. Number-theoretic algorithms in cryptography / O. N. Vasilenko. – M.: MTSNMO, 2003. – 328 p.
4. Gultyaeva T. A. Fundamentals of information theory and cryptography. – Novosibirsk: NGTU Publishing House, 2010. – 88 p. – ISBN 978-5-7782-1425-5.
5. Denisenko D.V., Marshalko G.B., Nikitenkova M.V., Rudskoi V.I., Shishkin V.A. Evaluation of the complexity of the implementation of the Grover algorithm for enumerating the keys of block cipher algorithms GOST R 34.12-2015, Journal of Experimental and Theoretical Physics, Russian Academy of Sciences, Institute of Physical Problems. P.L. Kapitsa RAS (Moscow), 2019, volume 155, no. 4, pp. 645–653, 2019.
6. Kitaev A., Shen A., Vyaly M. Classical and quantum computing / M.: MTsNMO, Izd. CheRo, 1999. – 192 p.
7. Kolmogorov, A.N. Information theory and theory of algorithms. Academy of Sciences of the USSR. – M.: Nauka, 1987.
8. Kotelnikov V. A. Fate that embraced the age. In 2 tons / comp. N. V. Kotelnikova. M.: Fizmatlit, 2011. – 312 p.
9. Korolkov A.V. On some applied aspects of quantum cryptography in the context of the development of quantum computing and the emergence of quantum computers. / A.V. Korolkov // Cybersecurity Issues No. 1(9) – 2015. – M .: Journal «Cybersecurity Issues», 2015. – pp. 6-13.
10. Klyucharev P.G. Abstract of the dissertation for the competition of a candidate of technical sciences. Algorithmic and software for quantum computer simulation. MSTU im. N.E. Bauman, 2009, 18 p.
11. Crandall R., Pomerance K. Prime numbers: Cryptographic and computational aspects / ed. V. N. Chubarikov; per. A. V. Begunts [i dr.]. – M.: URSS: Book house «LIBROKOM», 2011. – 664 p.
12. Manin Yu.I. Computable and non-computable. M.: Soviet radio, 1980. 128 p.
13. Matveev E.A. Dissertation for the Candidate of Physical and Mathematical Sciences. Application of quantum mechanical effects in information security systems. Penza, NTP Cryptosoft, 2019 – 157 p. 5.
14. Moldovyan A.A., Moldovyan N.A. New forms of the hidden problem of discrete logarithm. Proceedings of SPIIRAS 2019. Volume 18 No. 2. Page 504-529.
15. Moldovyan N.A., Introduction to public key cryptosystems/ Moldovyan N.A., Moldovyan A.A./, Ed. BHV-Petersburg, 2005, 286 p. – 2005.
16. Nikolenko S.I. New constructions of cryptographic primitives based on semigroups, groups and linear algebra. Dissertation for the Candidate of Physical and Mathematical Sciences. St. Petersburg, Institution of the Russian Academy of Sciences St. Petersburg Department of the Mathematical Institute. V.A. Steklov RAS, 2008 – 120 p.
17. Nielsen M., Chang I. Quantum Computing and Quantum Information. Per. from English – M: Mir, 2006 – 824 p., ill.
18. Fundamentals of cryptography. Textbook / A.P. Alferov [and others]. – M. : Helios ARV, 2001. – 480 p. — ISBN 5-85438-137-0.
19. Petrenko, A.S., Romanchenko A.M. A promising method of cryptanalysis based on the Shor algorithm // Protection of information. Inside No. 2 2020. – St. Petersburg: Ed. Athena, 2020. – p. 17–23.
20. Pravilshikov P.A. Quantum parallelism and solution of equations in control problems based on a new computational model / P.A. Pravilshikov. – M.: Institute of Management Problems. V.A. Trapeznikova, 2014.- 179 p.
21. Preskill J. Quantum information and quantum computing / D. Preskill.-M.: Izhevsk, 2008. – 464 p.
22. Ruchkin V.N. Natural parallelism of quantum computers and neurocomputers / V.N. Ruchkin, V.A. Romanchuk, V.A. Fulin.- Ryazan: Ryazan State University. S.A. Yesenina, 2013 – 387 p.
23. Sachkov V.N., V.A. Kotelnikov and encrypted communication. Conferences and Symposiums, Vol. 176, No. 7, UFN 2006, p. 775-777
24. Dictionary of cryptographic terms. Edited by B. A. Pogorelov and V. N. Sachkov. Moscow State University M.V. Lomonosov Academy of Cryptography of the Russian Federation. Moscow MTsNMO publishing house. 2006. – 50 p.

25. Tokareva N.N. On the history of cryptography in Russia, Historical essays on discrete mathematics and its applications, No. 4 (18), Mathematical Institute. S.L. Sobolev SB RAS, Novosibirsk, 2012, – p. 82-107.
26. Holevo A. S. Mathematical foundations of quantum informatics – M.: MIAN, 2018. – 118 p. – (Lec. courses of REC, ISSN 2226-8782; Issue 30). ISBN 978-5-98419-080-7
27. Holevo A. S., Quantum Systems, Channels, Information. Electronic edition. M.: MTSNMO, 2014. – 327 p. ISBN 978-5-4439-2092-4
28. Holevo A. S., Introduction to quantum information theory. MTSNMO, 2002 – 128 p. 10.
29. Cheryomushkin A. V. Cryptographic protocols: basic properties and vulnerabilities // Applied Discrete Mathematics. – 2009. – Nov. – vol. 2. – p. 115-150. – URL: https://cyberleninka. ru / article / n / kriptograficheskie – protokoly-osnovnye-svoystva-i-uyazvimosti.pdf.
30. Shannon K. Works on information theory and cybernetics / ed. R. L. Dobrushina, O. B. Lupanova. – M.: Publishing house of foreign literature, 1963. – 830 p.
31. Schneier B. Applied cryptography: protocols, algorithms, source code in C. Ed. Williams, 2016. 816p.
32. Shor P. Algorithms for quantum computation: discrete logarithms and factoring [Text] / Shor P.// Foundations of Computer Science.—1994.—No. 10. -134p.
33. Deutsch D., Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society A. 400 (1818), 97-117 (1985)
34. Deutsch D., Jozsa R., Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London A, 439, (1907), 553-558 (1992)
35. Diffie D, Hellman M. New directions in cryptography, IEEE Transactions on Information Theory, v. 22, Issue 6 (1976)
36. Feynman R, Simulating physics with computers, Internat. J. Theoret. Phys. 21, 467-488 (1982)
37. Grover L.K., A fast quantum mechanical algorithm for database search, In Proceedings of the twenty-eighth, annual ACM symposium on Theory of computing, 212 – 219, ACM (1996)
38. Markov A., Markov G., Tsirlov V. SIMULATION OF SOFTWARE SECURITY TESTS BY SOFT COMPUTATIONAL METHODS: CRITICAL INFRASTRUCTURES: CONTINGENCY MANAGEMENT, INTELLIGENT, AGENT-BASED, CLOUD COMPUTING AND CYBER SECURITY (IWCI 2019). Proceedings of the VIth International Workshop. Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences. 2019. С. 257-261.
39. Dorofeev A.V., Markov A.S., Tsirlov V.L. APPLICATION OF OPEN DATA IN ACCORDANCE WITH INFORMATION SECURITY REQUIREMENTS: CEUR Workshop Proceedings. ISTMC 2019 – Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation «Information Systems and Technologies in Modeling and Control». 2019. С. 36-46.
40. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing 26, 1484 – 1509 (1997).
41. Simon D.R., On the power of quantum computation, SFCS ‹94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 116 – 123 (1994).